Listing of Claims

Claim 1. (Original) In a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M" obtained by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I and by supplying the cyphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom, a method by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the cyphertext message M comprising the steps of:

a. the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities;

b. the sending unit S:

i. retrieving the plurality of public quantities from the publicly accessible repository;

ii. using at least some of the plurality of public quantities, computing and transmitting to the

receiving unit R a plurality of sender's quantities; and

iii. using at least one of the plurality of public quantities, computing the key K; and

c. the receiving unit R, using at least one of the plurality of sender's quantities received from the sending unit S computing the key K.

Claim 2. (Original) The method of claim 1 wherein the receiving unit R, in storing the plurality of public quantities into the publicly accessible repository:

i. selects at least one receiver's secret quantity;

ii. selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and

iii. using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

Claim 3. (Original) The method of claim 2 wherein the plurality of public quantities include a plurality of vectors.

Claim 4. (Original) The method of claim 2 wherein the at least one selected public quantity includes a vector.

Claim 5. (Original) The method of claim 2 wherein the plurality of computed public quantities include a plurality of vectors.

Claim 6. (Original) The method of claim 2 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities.

Claim 7. (Original) The method of claim 6 wherein the plurality of sender's quantities include a plurality of vectors.

Claim 8. (Original) The method of claim 1 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities.

Claim 9. (Original) The method of claim 8 wherein the plurality of sender's quantities include a plurality of vectors.

Claim 10. (Original) A system adapted for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

a. a communication channel I adapted for transmitting the cyphertext message M;

b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I; and

c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, each cryptographic unit:

i. when the cryptographic unit is to receive the cyphertext message M:

(1) storing plurality of public quantities in a publicly accessible repository;

(2) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit, and using at least one of the plurality of sender's quantities in computing the key K; and

ii. when the cryptographic unit is to send the cyphertext message M, retrieving the plurality of public quantities from the publicly accessible repository and using:

(1) at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit; and

(2) at least one of the plurality of public quantities in computing the key K; and

iii. including a cryptographic device having:

(1) a key input port for receiving the key K from the cryptographic unit;

(2) a plaintext port:

(a) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device, and

(b) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and

(3) a cyphertext port that is coupled to one of said transceivers:

(a) for transmitting the cyphertext message M to such transceiver, and

(b) for receiving the cyphertext message M from such transceiver.

Claim 11. (Original) The system of claim 10 wherein said cryptographic unit which receives the cyphertext message M in

storing the plurality of public quantities into the publicly accessible repository:

(a) selects at least one receiver's secret quantity;

(b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and

(c) using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

Claim 12. (Original) The system of claim 11 wherein the plurality of public quantities include a plurality of vectors.

Claim 13. (Original) The system of claim 11 wherein the at least one selected public quantity includes a vector.

Claim 14. (Original) The system of claim 11 wherein the plurality of computed public quantities include a plurality of vectors.

Claim 15. (Original) The system of claim 11 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit::

i. selects a sender's secret quantity;; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

Claim 16. (Original) The system of claim 15 wherein the plurality of sender's quantities include a plurality of vectors.

Claim 17. (Original) The system of claim 10 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

i. selects a sender's secret quantity;; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

Claim 18. (Original) The system of claim 17 wherein the plurality of sender's quantities include a plurality of vectors.

Claim 19. (Original) A cryptographic unit adapted for inclusion in a system for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system including:

a. a communication channel I adapted for transmitting the cyphertext message M; and

b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I;

the cryptographic unit being adapted for coupling to said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, and comprising:

a. ports:

i. when the cryptographic unit is to receive the cyphertext message M, for:

(1) storing plurality of public quantities in a publicly accessible repository;

(2) receiving via the communication channel I a plurality of sender's quantities from a send-

ing cryptographic unit, and using at least one of the plurality of sender's quantities in computing the key K; and

ii. when the cryptographic unit is to send the cyphertext message M, for retrieving the plurality of public quantities from the publicly accessible repository and using:

(1) at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit; and

(2) at least one of the plurality of public quantities in computing the key K; and

b. a cryptographic device having:

i. a key input port for receiving the key K from the cryptographic unit;

ii. a plaintext port:

(1) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device, and

(2) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and

ii. a cyphertext port that is coupled to one of said transceivers:

(1) for transmitting the cyphertext message M to such transceiver, and

(2) for receiving the cyphertext message M from such transceiver.

Claim 20. (Original) The cryptographic unit of claim 19 wherein, when receiving the cyphertext message M, in storing the plurality of public quantities into the publicly accessible repository:

(a) selects at least one receiver's secret quantity;

(b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and

(c) using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as

part of the plurality of public quantities a plurality of computed public quantities.

Claim 21. (Original) The cryptographic unit of claim 20 wherein the plurality of public quantities include a plurality of vectors.

Claim 22. (Original) The cryptographic unit of claim 20 wherein the at least one selected public quantity includes a vector.

Claim 23. (Original) The cryptographic unit of claim 20 wherein the plurality of computed public quantities include a plurality of vectors.

Claim 24. (Original) The cryptographic unit of claim 20, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving

cryptographic unit the plurality of sender's quantities.

Claim 25. (Original) The cryptographic unit of claim 24 wherein the plurality of sender's quantities include a plurality of vectors.

Claim 26. (Original) The cryptographic unit of claim 19 wherein, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

i. selects a sender's secret quantity; and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

Claim 27. (Original) The cryptographic unit of claim 26 wherein the plurality of sender's quantities include a plurality of vectors.

Claim 28. (Currently amended) In a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and, wherein before transmitting the message M and the digital signature, the sending unit S transmits for storage in a publicly accessible repository ~~a plurality of public quantities~~ a large integer n and three (3) vectors, a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:

a. retrieving the ~~plurality of public quantities~~ large integer n and the three (3) vectors from the publicly accessible repository;

b. using the digital signature and the ~~plurality of public quantities~~ large integer n and the three (3) vectors, evaluating expressions of at least two (2) different verification relationships; and

c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

Claim 29. (Canceled) ~~The method of claim 28 wherein the plurality of public quantities include a plurality of vectors.~~